	Type	Hits	Search Text	DBs	Time Stamp
1	IS&R	1549	(705/39,41,43,44,35,18,26).CCLS.	USPAT	2002/07/08 15:01
2	IS&R	492	(705/50,53,64,67,72,76,78,79).CCLS.	USPAT	2002/07/08 15:06
3	IS&R	184	(902/35,20,24,40).CCLS.	USPAT	2002/07/08 15:07
4	IS&R	344	(902/35,20,24,40,3,5).CCLS.	USPAT	2002/07/08 15:12
5	IS&R	213	(382/115).CCLS.	USPAT	2002/07/08 15:15
6	IS&R	2538	(235/379,380).CCLS.	USPAT	2002/07/08 15:24
7	IS&R	7	(("5371797") or ("5577120") or ("5794207") or ("6023688") or ("6052675") or ("6260024") or ("6327578")).PN.	USPAT	2002/07/08 15:25

updated search

DIALOG SEARCH
09 July 2002

File 9:Business & Industry(R) Jul/1994-2002/Jul 05
(c) 2002 Resp. DB Svcs.
File 623:Business Week 1985-2002/Jul 08
(c) 2002 The McGraw-Hill Companies Inc
File 810:Business Wire 1986-1999/Feb 28
(c) 1999 Business Wire
File 275:Gale Group Computer DB(TM) 1983-2002/Jul 04
(c) 2002 The Gale Group
File 624:McGraw-Hill Publications 1985-2002/Jul 08
(c) 2002 McGraw-Hill Co. Inc
File 813:PR Newswire 1987-1999/Apr 30
(c) 1999 PR Newswire Association Inc
File 636:Gale Group Newsletter DB(TM) 1987-2002/Jul 04
(c) 2002 The Gale Group
File 621:Gale Group New Prod.Annou.(R) 1985-2002/Jul 04
(c) 2002 The Gale Group
File 16:Gale Group PROMT(R) 1990-2002/Jul 04
(c) 2002 The Gale Group
File 148:Gale Group Trade & Industry DB 1976-2002/Jul 05
(c)2002 The Gale Group
File 20:Dialog Global Reporter 1997-2002/Jul 09
(c) 2002 The Dialog Corp.
File 610:Business Wire 1999-2002/Jul 09
(c) 2002 Business Wire.
File 613:PR Newswire 1999-2002/Jul 09
(c) 2002 PR Newswire Association Inc
File 348:EUROPEAN PATENTS 1978-2002/Jun W05
(c) 2002 European Patent Office
File 349:PCT FULLTEXT 1983-2002/UB=20020627,UT=20020620
(c) 2002 WIPO/Univentio
File 625:American Banker Publications 1981-2002/Jul 09
(c) 2002 American Banker
File 268:Banking Info Source 1981-2002/Jun W5
(c) 2002 ProQuest Info&Learning
File 626:Bond Buyer Full Text 1981-2002/Jul 09
(c) 2002 Bond Buyer
File 267:Finance & Banking Newsletters 2002/Jul 08
(c) 2002 The Dialog Corp.
File 139:EconLit 1969-2002/Jun
(c) 2002 American Economic Association
File 608:KR/T Bus.News. 1992-2002/Jul 09

Set Items Description
S1 60634 (BIOMETRIC OR FINGER? OR IRIS OR RETINA? ? OR FACE? ? OR V-
OICE? ?)(4N)(PATTERN? ? OR PRINT? OR SIGNATURE? OR CHARACTERI-
STIC? OR SCAN?)
S2 7504 S1(4N)(VERIFIC? OR VERIFY? OR AUTHENTICAT? OR VALIDAT? OR -
IDENTIFY? OR IDENTIFIED OR COMPAR? OR MATCH?)
S3 521 S2(S)((ELECTRONIC OR DIGITAL OR FINANCIAL)(2N)TRANSACTION?
? OR E(2N)COMMERCE OR ELECTRONIC(2N)COMMERCE)
S4 22 S2(4N)((ELECTRONIC OR DIGITAL OR FINANCIAL)(2N)TRANSACTION?
? OR E(2N)COMMERCE OR ELECTRONIC(2N)COMMERCE)
S5 14 RD S4 (unique items)
S6 120 S3 NOT PY>1999
S7 63 RD S6 (unique items)

considered all (AB, KWIC)

01350301 00-01288

ID at touch of a finger

Yamada, Ken

Computer Reseller News n713 PP: 93-95 Dec 2, 1996 ISSN: 0893-8377
JRNL CODE: CRN
DOC TYPE: Journal article LANGUAGE: English LENGTH: 2 Pages
WORD COUNT: 573

ABSTRACT: The National Registry Inc. has introduced a new generation of fingertip scanning solutions. They are available in 2 configurations, both of which are based on optical technology. The scanners are used in conjunction with NRI software loaded locally on PCs or on servers running Windows software. There are 2 types of identification procedures used by NRI - verification and certification.

TEXT: Headnote:

New scanning solutions hit mainstream

IDENTIFICATION made through fingertip scanning no longer is a technology limited to operations of the cloak-and-dagger variety.
The cost of fingertip scanning technology has dropped to a price affordable for corporate enterprises and vertical applications, said Clint Fuller, vice president of marketing at The National Registry Inc. (NRI), St Petersburg, Fla.

The price of fingertip scanning solutions may be implemented for as low as $500 a workstation, compared with $2,500 a workstation a year ago, Fuller said.

NRI launched a new generation of fingertip scanning solutions. They are available in two configurations, which include either a desktop scanner in the size and shape of a standard PC mouse or a scanner built into a keyboard. Both units are based on optical technology. The scanners are used in conjunction with NRI software loaded locally on PCs or on servers running Windows software.

"Security has become important in all aspects of computer networks," Fuller said. "If you can never positively identify a user of the system, then all of the other security measures don't matter." For most people, he said, security means just the use of a password.

Overall, Fuller said, fingertip scanning serves to eliminate the weakest links in a security chain, which include passwords.

To use the technology, an image of a person's fingertip is captured by a scanner. That image is analyzed by the computer for unique features called "minutiae, creating a unique fingerimage identifier number. The fingerimage is compared with other identifier numbers stored in a database.

NRI said applications well-suited for **fingertip scanning** include **authenticating** the initiator of **electronic transactions** such as funds transfers, security trades and credit purchases. They also include identifying individuals in computer-based enrollment for new account openings, insurance applications, membership in professional organizations and social services.

The banking, heath care and travel industries may benefit from fingertip scanning by making possible the convenient, fast and positive identification of customers, NRI said.

NRI works with VARs to target many of these vertical markets, Fuller said.

NRI priced its keyboard scanner at $420 and its mouse-size scanner at $390. Both include a small box connected to the PC that acts as a "frame

grabber."

NRI's software comes in a variety of packages, including a pre-configured PC solution priced at $500, plus a $100 license fee per PC.

A software developer's kit for integrating the technology into an application is priced at $1,000, plus a $200 per PC licensing fee.

Server-based software is priced at $5,000 for a basic solution and $35,000 for a high-end solution used by organizations such as welfare agencies.

NRI's scanners are manufactured by Key Tronic corp., spokane, Wash., through an agreement made last year.

Production units of the scanners were due out in November. Prototypes of the scanners already have been implemented by a variety of companies, including hospitals, software vendors and a network service provider, NRI said.

There are two types of identification procedures used by NRIverification and certification.
Verification answers a one-to-one match that verifies people's identities.

Certification is a one-to-many match that checks one person's identity under various names.

Enrollment is the process of entering a new identifier into the database. The finger image may be provided by a live scan of an individual's fingertip, or by scanning an inked fingerprint on paper. Enrollment typically begins with a one-to-many certification match to make sure that the enrollee is not in the database under another name.

COMPANY NAMES:
National Registry Inc
GEOGRAPHIC NAMES: US

DESCRIPTORS: Identification systems; Fingerprinting; Scanners; Product introduction
CLASSIFICATION CODES: 9190 (CN=United States); 8650 (CN=Electrical & electronics industries); 9120 (CN=Product specific)
?

5/9/3 (Item 1 from file: 9)
DIALOG(R)File 9:Business & Industry(R)

02467051 (THIS IS THE FULLTEXT)
LCI Intros SMARTpen Biometric Signature Authentication
(LCI Technology has introduced SMARTpen, a biometric signature authentication system that is wireless)
Newsbytes News Network, p N/A
May 24, 1999
DOCUMENT TYPE: Journal (United States)
LANGUAGE: English RECORD TYPE: Fulltext
WORD COUNT: 345

TEXT:
S'HERTGENBOSCH, NETHERLANDS, 1999 MAY 24 (NB) -- By Sylvia Dennis, Newsbytes. LCI Technology has taken the wraps off its SMARTpen biometric signature authentication system. The SMARTpen is billed as the world's first wireless signature device and the only biometric unit of its type that writes on normal paper.

Sam Asseer, the firm's chairman, said that the unit was designed for high-end security transactions. It is, he explained, a wireless embedded computer system that looks and writes like a common ballpoint pen. In use, the SMARTpen uses built-in sensors that enable the **authentication** of users through the **biometric characteristics** of their **signatures** on regular paper.

" **Electronic commerce** is rapidly becoming the way the world does business," he said, adding that the surge in online transactions over the past two years and the predictions for explosive growth going into the year 2000 suggests that the future of e-commerce is unlimited.

"But, as the number of Internet transactions increases, there is an even greater demand for security to ensure confidentiality and prevent fraud. Biometric authentication systems like the LCI SMARTpen help create the secure environment necessary for the continued expansion of global e-commerce," he said.

According to the firm, the SMARTpen measures individual signature characteristics, encrypts the data and transmits it via radio frequency to a computer, where LCI software compares it to a template for verification - all in about three seconds.

The firm claims that the dynamics of signatures as measured by the SMARTpen are personal and not directly visible from the written image. This, the firm says, makes it virtually impossible for forged signatures to get through the SMARTpen system. The system works with standard APIs (application programming interfaces) and the false rejection/false acceptance rate can be adjusted by system parameters, so adding flexibility.

Pricing on the SMARTpen is expected to range from $100 to $250, depending on the model and configuration of the product.

According to LCI, the price includes the pen and software components. The SMARTpen also has integral sensors, a mouse, a digital signal processor, radio transmitter and receiver, and encryption system.

COMPANY NAMES: LCI TECHNOLOGY
INDUSTRY NAMES: Computer; Telecom equipment; Telecommunications
PRODUCT NAMES: Pen-based input devices (357754); Alarm systems and other security equipment (366923)
CONCEPT TERMS: All product and service information; Product introduction
GEOGRAPHIC NAMES: North America (NOAX); United States (USA)
?

01430692 00-81679

Internet security: A technical report

Walsh, Bob

Texas Banking v86n5 PP: 16-17 May 1997 ISSN: 0885-6907 JRNL CODE: TXB
DOC TYPE: Journal article LANGUAGE: English LENGTH: 2 Pages
WORD COUNT: 911

ABSTRACT: Secure transactions on the Internet involve 3 objectives: 1. encryption, 2. integrity assurance, and 3. authentication. These 3 objectives of secure Internet communication are implemented by the use of security proposals. The 2 most popular are Secure Sockets Layer, developed by Netscape Communications Corp., and Private Communication Technology, written by Microsoft Corp. These protocols use symmetric key and asymmetric key cryptography to ensure security.

TEXT: Electronic commerce made possible by the Internet presents any organization with a major decision.

This is especially true of Internet banking. On one hand, competition demands that you offer this service to your customers and offer it soon, but the issue of security on the Internet demands that you proceed slowly and cautiously.

Horror stories of company identities being used to collect credit card data and reports proclaiming that the security key for a popular encryption protocol was decoded get top headlines in newspapers around the world.

These stories fuel our fear of performing financial transactions on the Internet. Is the Internet the "black hole of security" that we hear about in all the trades or just a perception based on misinformation?

Security breaches on the Internet are certainly the exception rather than the rule. Consider this fact: Netscape Communications has had over eight million customers doing business on the Internet for almost a year and have had no reports from any of those customers about information being stolen.

Closer to home, banks surveyed by a member of the Gartner Group, a well-known information technology firm, report that they have never seen a credit card number stolen during an Internet transmission.

Even so, you are still not sure if the Internet is safe enough for commerce or your customer's bank records. The purpose of this article is to explain how to transmit sensitive information safely over the Internet. These technologies are in use today and are the basis of a prudent security approach for secure Internet transactions. Secure transactions on the Internet involve three objectives:

Encryption -- Scrambling data so it is unusable if intercepted;

Integrity Assurance - Assuring that received data has not been altered in transit; and Authentication -- Verifying a message's origin and the sender's identity.

These three objectives of secure Internet communication are implemented by the use of security protocols. The two most popular are Secure Sockets Layer (SSL), developed by Netscape Communications Corporation and Private Communication Technology (PCT), written by Microsoft Corporation.

While each has certain unique features, both accomplish the same job. SSL appears to be more widely used and Microsoft has built SSL compatibility into all of its Internet products.

These protocols use symmetric key and asymmetric key cryptography to ensure security.
Symmetric key, uses just one file cryptography, which is the basis for the

secure method of encryption key, uses just one file the only way encrypt and decrypt messages. This is a very secure method of encryption since the only way to "crack" the code in the file is to perform "brute force" calculations -try every possible combination of factors - to decipher it. The file is so large that brute force solutions take longer to determine than the life of the file.

Using this type of security alone is cumbersome because the delivery of the file must be accomplished by secure means such as a courier.

Asymmetric key cryptography uses two decoder files. One file is shared freely while the other is never divulged. Since the freely shared file can only be used to encrypt a message, the need to send it by a secure means is eliminated. This is the basis for the beginning steps of a secure transaction.

Here is the basic "conversation" that occurs between an Internet browser and server to set up a secure channel on which to pass information:

The client (customer) sends a request to send data securely. The server responds by sending a certificate, which is issued by a recognized certificate authority. This includes information about the server's owner and the server's freely shared encryption file or public key.

The client verifies that the certificate is valid by contacting the issuer of the certificate if necessary, creates a unique session key and sends it back to the server encrypted with the server's freely shared encryption file.

The server decrypts the session key with its private key file.

Subsequent messages during the session are encrypted using a mutually agreed upon encryption algorithm and the session key.

This security method is sufficient for most of the secure transactions that occur on the Internet. New methods are being developed and refined all the time.

One change requires that the client have a certificate too. This would ensure that the customer is who he says he is and not rely on just a user ID and password. Additional upgrades to security on the Internet are also being tested. One such security method, biometrics, automated methods of establishing someone's identity from their unique physiological or behavioral characteristics, is being tested in several financial institutions in the United States and is already in use around the world.

(Illustration Omitted)

Captioned as: Steps to Connect to a Secure Internet Server

The most common method is a finger scan. The customer swipes his bank card and has a **fingerprint scanned** . This information is **compared** to a database and access is granted if there is a match. Applications using this technology on the Internet are not far off While no method of security except complete system isolation is absolute, these methods should give most customers and financial institutions a more secure feeling about performing **financial transactions** on the Internet. Encryption, authentication, and data integrity security methods exist now. Properly implemented, these protocols should eliminate the uncertainty associated with Internet **financial transactions** . U

Author Affiliation:

AdAstra Technologies Inc. is a TBA associate member that assists financial institutions in implementing technology to help stay competitive.

GEOGRAPHIC NAMES: US

DESCRIPTORS: Electronic commerce; Internet; Data encryption; Protocol

CLASSIFICATION CODES: 919[redacted](CN=United States); 5250 (CN=Te[redacted]communications systems); 5140 (CN=Security)
?

7/9/38 (Item 3 from f[redacted]: 16)
DIALOG(R)File 16:Gale Gr[redacted]p PROMT(R)

01384372 Supplier Number: 41645883
BIOMETRIC SYSTEMS OPEN THE DOOR
Mechanical Engineering-CIME, p58
Nov, 1990
ISSN: 0025-6501
Language: English Record Type: Abstract
Document Type: Magazine/Journal; Refereed; Trade

ABSTRACT:
Biometric systems are attaining a new degree of protection in fraud prevention and security-control devices via **verifying** unique personal features including **signatures** , **retinal** blood vessel **patterns** , **fingerprints** and speech. The practical employment of biometric systems is now limited to verification. Verification means that the machine accepts or rejects the claim of an unidentified person; it does not identiffy users who are not involved within a set of reference samples. A basis of a biometric verfifier is exmaining the dynamics of the way a person signs one's name. Future users for that kind of system include verifying credit card signatures and automatic teller machine **transactions** including the **electronic** transfer of bank funds. Detail is given to the biometric system efforts of IBM's Thomas J Watson Research Center (Yorktown Hts, NY), Autosig Systems (Irving, TX), Eyedentify (Portland, OR), Recognition Systems (San Jose, CA), Ecco Industries (Danvers, MA) and Sandia Natl Labs (Albuquerque, NM).

PUBLISHER NAME: American Society of Mechanical Engineers
EVENT NAMES: *330 (Product information)
GEOGRAPHIC NAMES: *1USA (United States)
PRODUCT NAMES: *3662300 (Intercom, Signal & Alarm Eqp); 3579910 (Access ID Card Equipment)
INDUSTRY NAMES: BUSN (Any type of business); ENG (Engineering and Manufacturing)
NAICS CODES: 33429 (Other Communications Equipment Manufacturing); 334119 (Other Computer Peripheral Equipment Manufacturing)
?

5/9/3 (Item 1 from f : 9)
DIALOG(R)File 9:Business & Industry(R)

02467051 (THIS IS THE FULLTEXT)
LCI Intros SMARTpen Biometric Signature Authentication
(LCI Technology has introduced SMARTpen, a biometric signature authentication system that is wireless)
Newsbytes News Network, p N/A
May 24, 1999
DOCUMENT TYPE: Journal (United States)
LANGUAGE: English RECORD TYPE: Fulltext
WORD COUNT: 345

TEXT:
S'HERTGENBOSCH, NETHERLANDS, 1999 MAY 24 (NB) -- By Sylvia Dennis, Newsbytes. LCI Technology has taken the wraps off its SMARTpen biometric signature authentication system. The SMARTpen is billed as the world's first wireless signature device and the only biometric unit of its type that writes on normal paper.

Sam Asseer, the firm's chairman, said that the unit was designed for high-end security transactions. It is, he explained, a wireless embedded computer system that looks and writes like a common ballpoint pen. In use, the SMARTpen uses built-in sensors that enable the **authentication** of users through the **biometric characteristics** of their **signatures** on regular paper.

" **Electronic commerce** is rapidly becoming the way the world does business," he said, adding that the surge in online transactions over the past two years and the predictions for explosive growth going into the year 2000 suggests that the future of e-commerce is unlimited.

"But, as the number of Internet transactions increases, there is an even greater demand for security to ensure confidentiality and prevent fraud. Biometric authentication systems like the LCI SMARTpen help create the secure environment necessary for the continued expansion of global e-commerce," he said.

According to the firm, the SMARTpen measures individual signature characteristics, encrypts the data and transmits it via radio frequency to a computer, where LCI software compares it to a template for verification - all in about three seconds.

The firm claims that the dynamics of signatures as measured by the SMARTpen are personal and not directly visible from the written image. This, the firm says, makes it virtually impossible for forged signatures to get through the SMARTpen system. The system works with standard APIs (application programming interfaces) and the false rejection/false acceptance rate can be adjusted by system parameters, so adding flexibility.

Pricing on the SMARTpen is expected to range from $100 to $250, depending on the model and configuration of the product.

According to LCI, the price includes the pen and software components. The SMARTpen also has integral sensors, a mouse, a digital signal processor, radio transmitter and receiver, and encryption system.

COMPANY NAMES: LCI TECHNOLOGY
INDUSTRY NAMES: Computer; Telecom equipment; Telecommunications
PRODUCT NAMES: Pen-based input devices (357754); Alarm systems and other security equipment (366923)
CONCEPT TERMS: All product and service information; Product introduction
GEOGRAPHIC NAMES: North America (NOAX); United States (USA)
?

01430692 00-81679

Internet security: A technical report

Walsh, Bob

Texas Banking v86n5 PP: 16-17 May 1997 ISSN: 0885-6907 JRNL CODE: TXB
DOC TYPE: Journal article LANGUAGE: English LENGTH: 2 Pages
WORD COUNT: 911

ABSTRACT: Secure transactions on the Internet involve 3 objectives: 1. encryption, 2. integrity assurance, and 3. authentication. These 3 objectives of secure Internet communication are implemented by the use of security proposals. The 2 most popular are Secure Sockets Layer, developed by Netscape Communications Corp., and Private Communication Technology, written by Microsoft Corp. These protocols use symmetric key and asymmetric key cryptography to ensure security.

TEXT: Electronic commerce made possible by the Internet presents any organization with a major decision.

This is especially true of Internet banking. On one hand, competition demands that you offer this service to your customers and offer it soon, but the issue of security on the Internet demands that you proceed slowly and cautiously.

Horror stories of company identities being used to collect credit card data and reports proclaiming that the security key for a popular encryption protocol was decoded get top headlines in newspapers around the world.

These stories fuel our fear of performing financial transactions on the Internet. Is the Internet the "black hole of security" that we hear about in all the trades or just a perception based on misinformation?

Security breaches on the Internet are certainly the exception rather than the rule. Consider this fact: Netscape Communications has had over eight million customers doing business on the Internet for almost a year and have had no reports from any of those customers about information being stolen.

Closer to home, banks surveyed by a member of the Gartner Group, a well-known information technology firm, report that they have never seen a credit card number stolen during an Internet transmission.

Even so, you are still not sure if the Internet is safe enough for commerce or your customer's bank records. The purpose of this article is to explain how to transmit sensitive information safely over the Internet. These technologies are in use today and are the basis of a prudent security approach for secure Internet transactions. Secure transactions on the Internet involve three objectives:

Encryption -- Scrambling data so it is unusable if intercepted;

Integrity Assurance - Assuring that received data has not been altered in transit;, and Authentication -- Verifying a message's origin and the sender's identity.

These three objectives of secure Internet communication are implemented by the use of security protocols. The two most popular are Secure Sockets Layer (SSL), developed by Netscape Communications Corporation and Private Communication Technology (PCT), written by Microsoft Corporation.

While each has certain unique features, both accomplish the same job. SSL appears to be more widely used and Microsoft has built SSL compatibility into all of its Internet products.

These protocols use symmetric key and asymmetric key cryptography to ensure security.
Symmetric key, uses just one file cryptography, which is the basis for the

secure method of encry on key, uses just one file the ly way encrypt and decrypt messages. Thi- is a very secure method of encr,ption since the only way to "crack" the code in the file is to perform "brute force" calculations -try every possible combination of factors - to decipher it. The file is so large that brute force solutions take longer to determine than the life of the file.

Using this type of security alone is cumbersome because the delivery of the file must be accomplished by secure means such as a courier.

Asymmetric key cryptography uses two decoder files. One file is shared freely while the other is never divulged. Since the freely shared file can only be used to encrypt a message, the need to send it by a secure means is eliminated. This is the basis for the beginning steps of a secure transaction.

Here is the basic "conversation" that occurs between an Internet browser and server to set up a secure channel on which to pass information:

The client (customer) sends a request to send data securely. The server responds by sending a certificate, which is issued by a recognized certificate authority. This includes information about the server's owner and the server's freely shared encryption file or public key.

The client verifies that the certificate is valid by contacting the issuer of the certificate if necessary, creates a unique session key and sends it back to the server encrypted with the server's freely shared encryption file.

The server decrypts the session key with its private key file.

Subsequent messages during the session are encrypted using a mutually agreed upon encryption algorithm and the session key.

This security method is sufficient for most of the secure transactions that occur on the Internet. New methods are being developed and refined all the time.

One change requires that the client have a certificate too. This would ensure that the customer is who he says he is and not rely on just a user ID and password. Additional upgrades to security on the Internet are also being tested. One such security method, biometrics, automated methods of establishing someone's identity from their unique physiological or behavioral characteristics, is being tested in several financial institutions in the United States and is already in use around the world.

(Illustration Omitted)

Captioned as: Steps to Connect to a Secure Internet Server

The most common method is a finger scan. The customer swipes his bank card and has a **fingerprint scanned** . This information is **compared** to a database and access is granted if there is a match. Applications using this technology on the Internet are not far off While no method of security except complete system isolation is absolute, these methods should give most customers and financial institutions a more secure feeling about performing **financial transactions** on the Internet. Encryption, authentication, and data integrity security methods exist now. Properly implemented, these protocols should eliminate the uncertainty associated with Internet **financial transactions** . U

Author Affiliation:

AdAstra Technologies Inc. is a TBA associate member that assists financial institutions in implementing technology to help stay competitive.

GEOGRAPHIC NAMES: US

DESCRIPTORS: Electronic commerce; Internet; Data encryption; Protocol

CLASSIFICATION CODES: 915 (CN=United States); 5250 (CN=Te communications systems); 5140 (CN=Security)
?

7/9/38 (Item 3 from f : 16)
DIALOG(R)File 16:Gale Group PROMT(R)

01384372 Supplier Number: 41645883
BIOMETRIC SYSTEMS OPEN THE DOOR
Mechanical Engineering-CIME, p58
Nov, 1990
ISSN: 0025-6501
Language: English Record Type: Abstract
Document Type: Magazine/Journal; Refereed; Trade

ABSTRACT:
Biometric systems are attaining a new degree of protection in fraud prevention and security-control devices via **verifying** unique personal features including **signatures** , **retinal** blood vessel **patterns** , **fingerprints** and speech. The practical employment of biometric systems is now limited to verification. Verification means that the machine accepts or rejects the claim of an unidentified person; it does not identiffy users who are not involved within a set of reference samples. A basis of a biometric verfifier is exmaining the dynamics of the way a person signs one's name. Future users for that kind of system include verifying credit card signatures and automatic teller machine **transactions** including the **electronic** transfer of bank funds. Detail is given to the biometric system efforts of IBM's Thomas J Watson Research Center (Yorktown Hts, NY), Autosig Systems (Irving, TX), Eyedentify (Portland, OR), Recognition Systems (San Jose, CA), Ecco Industries (Danvers, MA) and Sandia Natl Labs (Albuquerque, NM).

PUBLISHER NAME: American Society of Mechanical Engineers
EVENT NAMES: *330 (Product information)
GEOGRAPHIC NAMES: *1USA (United States)
PRODUCT NAMES: *3662300 (Intercom, Signal & Alarm Eqp); 3579910 (Access ID Card Equipment)
INDUSTRY NAMES: BUSN (Any type of business); ENG (Engineering and Manufacturing)
NAICS CODES: 33429 (Other Communications Equipment Manufacturing); 334119 (Other Computer Peripheral Equipment Manufacturing)
?